Lawsuits, downtime, data that has been stolen or destroyed—data insurance helps tech companies recoup unexpected losses.

data insurance

COVER YOUR MOST VALUABLE ASSETS—THE INTANGIBLE ONES

by Kevin Savetz

A business's most valuable asset isn't necessarily tangible. Perhaps it isn't a warehouse full of furniture, but a database of names, a directory of source code, an always-on Internet connection, or something equally ethereal. The owner of such a business might be surprised to find that none of these vital assets are covered by his or her insurance policy.

Traditional insurance products cover physical loss of tangible property. If a Web server is stolen or destroyed in a fire, the insurance company will pay to replace it. But all too often, the information stored on that server is worth much more than the hardware itself. But information isn't a tangible property, and regular insurance products aren't designed to cover that type of loss. For that, you need data insurance.

Data insurance, hacker insurance, or network security insurance—by any name, this type of coverage is a recent addition to insurance companies' offerings, and is relatively unknown among business owners. The idea is to protect the assets that are most valuable to e-businesses, such as electronic data and network connectivity.

We've all seen reports of stolen credit card databases in the news. These high-profile security breaches may be few and far between, but Internet security is a wide-scale problem for online businesses. And in the big picture, a stolen credit card file barely registers on the spectrum of bad stuff that can happen.

More than 52,000 Internet security incidents—in excess of 140 a day—were reported to the Computer Emergency Response Team Coordination Center (CERT/CC) in 2001, up from 21,000 in 2000. Those numbers are just a drop in the bucket. Most computer crimes aren't reported, and many more go undetected. When you consider that most hacking attempts are made by insiders, like

Illustration by Wesley Bedrosian.

disgruntled employees, the need for companies to prepare for risk becomes quite evident.

not your father's insurance policy

Although the data insurance sector is new, it's gaining popularity as companies learn the real risks of doing business on the Internet. Network security insurance is the fastest growing product in the history of insurance giant American International Group (AIG), according to Ty Sagalow, executive vice president and COO of AIG's eBusiness Risk Solutions. Bruce Schneier, CTO at Counterpane Internet Security, believes that sooner or later, it will be unthinkable not to have an anti-hacking policy.

But for the moment, choosing a policy—or even finding an insurance company that understands what it means to insure data—can be a challenge.

"Insurance products that deal with data insurance are emerging slowly," says Jack L. Strauss, president and CEO of SafeCorp, an information security consultancy. "There are few examples of standard products, and as such, their content from policy product to policy product varies greatly. Those that are offered in some standard fashion are over-constrained and ridiculously expensive. Also, the insurance industry as a whole moves at a glacial pace, even when they understand the target domain. And they don't get this space, as a group."

Counterpane's Schneier agrees. "There's more talk about this than actual policies being written." The market leader, AIG, claims 75 percent of the market. It has about 1,500 clients for its data insurance products, which have been available for two years.

How does a company determine whether it needs data insurance? "If, as a business, you don't use the Internet in any of your business operations—you don't have a Web site, you don't email outside the company, your computer room isn't connected to the outside world—then you don't need this insurance," Sagalow says. "But once you start using the Internet as part of your business strategy, the issue is not whether you need to buy this insurance for that risk, but rather, how much and what."

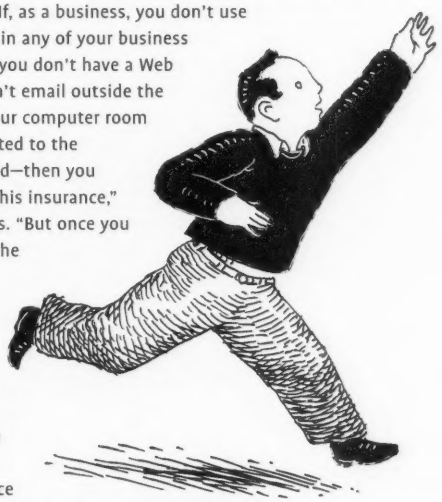


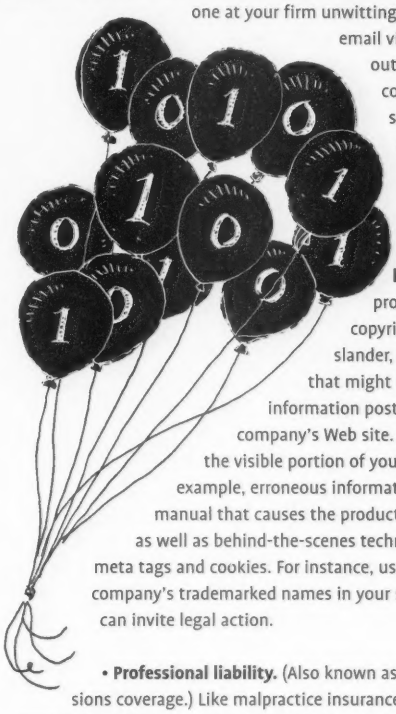
Illustration by Wesley Bedrosian.

coverage types

Shoppers will find many types of coverage under the broad umbrella of data insurance. When a business is connected to the Internet, the possibilities for damage go far beyond the "cracker breaks into your server and steals something of value" scenario that has been so often publicized by the evening news.

The major areas that a data insurance policy may cover include:

- **Legal liability to others.** This covers damage done to others as a result of security lapses on your network. For instance, if a cracker breaks into your network and uses your servers and routers to launch a denial of service attack on another company, or if some one at your firm unwittingly passes on an email virus to the outside world, this coverage would safeguard you against any resulting lawsuits.



- **Web content liability.** This protects against copyright, trademark, slander, and other suits that might result from information posted on your company's Web site. It can include the visible portion of your Web site—for example, erroneous information in an online manual that causes the product to explode—as well as behind-the-scenes technologies like meta tags and cookies. For instance, use of another company's trademarked names in your site's meta tags can invite legal action.

- **Professional liability.** (Also known as errors and omissions coverage.) Like malpractice insurance for doctors, errors and omissions coverage protects those who render professional services to others for a fee. It covers you if you're sued for rendering services in a negligent way. For example, if your company publishes content created by an outside contractor or freelancer, errors and omissions coverage will protect you if that content is inaccurate and causes enough problems to attract the interest of litigators.

- **Network security property loss.** This covers damage, corruption, or theft of data. For instance, if a hacker accesses your system and destroys, changes, or steals vital data. Such damage may not be immediately obvious. Some types of data corruption—an erased hard drive or modified home page—are meant to be noticed. Others, such as a former employee modifying data on a spreadsheet, may not be caught until much later.

- **Business interruption**. Coverage can compensate you for losses incurred when your site or network goes down. If your company sells books on the Internet and your site goes down, most customers won't wait to buy. Your competition is just a click away. This coverage can reimburse you for profits lost during the downtime.

- **Crisis communication.** During and following an Internet-related crisis, you may need to send the message to customers and shareholders that it's still safe to do business with you. Some insurance plans include crisis communication coverage to defray the expenses of PR agents and attorneys.

An insurer should let you pick and choose the types of coverage that your business needs. "If you don't have revenue associated with your site, you don't need business interruption service. If you don't have data that you're concerned about being corrupted, then you don't need damage insurance," Sagalow says.

The most common claims at AIG, according to Sagalow, are related to Web content liability, professional liability, and security. Part of this is because of the policy choices themselves. For instance, every one of AIG's offerings includes Web content liability coverage.

getting insured

Currently, data insurance mostly covers medium and large-size businesses. "What you're not likely to see for the next three years, at least, is a set of scalable insurance products that small to medium-size businesses will be able to understand and afford," SafeCorp's Strauss says.

The process of acquiring data insurance isn't that different from obtaining health insurance: Fill out some forms, then let a doctor check you out. The first step is to complete an insurance application, which includes questions about the technology products and services you use, and the people who manage the risks that you want to cover.

The second step is often an online security assessment, during which the CTO answers more detailed questions about the company's networking policies and procedures. Those two documents go to the underwriter, who may offer a quote. The insurance company might ask for an on-site security audit, which means that experts will interview employees and even attempt basic network intrusion techniques.

What will it cost to insure your data? That depends on many variables, including the type of insurance you choose, the amount of liability you have, the size of your company, and the security procedures your company has in place. "It would be fair to say that I have clients that spend as little as a few thousand dollars a year, and I have clients that spend hundreds of thousands a year," Sagalow says.

Determining the value of the data you want insured may not be easy. A single database or secret recipe may be the heart of your business, and estimating the worth of that intangible asset is a problem that can give CFOs nightmares.

"Until the insurance customers—enterprises, businesses, infrastructure suppliers, etcetera—can do a much better job of quantifying the value of stuff, for real, then we don't deserve better from the insurance guys," Strauss says.

You can likely get a discount on insurance premiums depending on the technologies you use. For instance, AIG gives discounts to businesses that use the eTrust software suite from Computer Associates, RSA SecurID to factor authentication, and the security assessment services of Unisys or Internet Security Systems.

"Eventually, the insurance industry will subsume the computer security industry," Schneier says. "The kind of firewall you use—along with the kind of authentication scheme you use, the kind of operating system you use, and the kind of network monitoring scheme you use—will be strongly influenced by the constraints of insurance. What will happen when the CFO realizes he can cut his insurance premium in half if he gets rid of all his insecure Windows OSs and replaces them with a hardened version of Linux? The choice of which OS to use will no longer be 100 percent technical."

Practices regarding the confidentiality of customer information are largely unregulated in the United States, at least at the federal level. There are exceptions, however, that are usually aimed at specific industries. For instance, the Gramm-Leach-Bliley Act

data insurance choices

Major providers of data insurance include:

American International Group
www.aignetadvantage.com
AIG offers a suite of coverage choices that include: Web content liability, professional errors and omissions, network security liability, cyber-extortion, Net security property loss, network security business interruption coverage, and crisis communication management. Policies have a $25 million capacity. For more information call (866) 638-2384.

The Hartford Financial Services Group
(www.thehartford.com)
The Hartford's "CyberFlex" policy is available to companies that have incidental exposures to cyber risks—for example, architectural firms. The policy doesn't currently offer coverage for technology and dot-com companies. Coverage includes Internet-related personal and advertising injury, electronic vandalism, Web site income, denial of service attacks, and good faith advertising. Policies are sold by independent agents, a list of agents is available on the Web site.

InsureTrust
www.insuretrust.com/insurance.html
InsureTrust offers electronic information errors and omissions liability, a third-party liability product with a $25 million capacity. Businesses can choose from among three coverage areas: professional liability, media and intellectual property offenses, and breach of computer security. You can fill out an application online or contact Steve Haase, CEO, at (770) 200-8035 or haase@insuretrust.com.

The St. Paul Companies
www.stpaul.com
The fifth largest commercial lines insurer in the country, The St. Paul Companies offers three technology products: Technology Internet Liability Protection, which provides claims-made liability coverage for "wrongful acts" committed on or through the Internet; Technology Network Security Protection, which provides coverage for first-party losses arising from network security issues; and Technology Errors and Omissions Liability Protection. Coverage limits range from $1 to $25 million. Contact Jon Farber, assistant vice president for technology, at jon.farber@stpaul.com or (651) 310-8366.

—KS

This is risk mitigation, not risk elimination. You can't get down to zero risk. An e-policy will help you deal with the risk you cannot eliminate.

focuses on privacy rules for financial institutions, the 1996 Health Insurance Portability and Accountability Act affects the medical industry, and the Children's Online Privacy Protection Act aims to protect children's privacy. Many states add their own privacy laws to the mix.

choosing an insurer

When choosing an insurer, look for one that has a specialized e-business unit and underwriters who understand the technical issues involved in data loss and Internet security. Look for a company with global reach. Sagalow suggests looking for carriers with a high capacity—the maximum amount of liability they will put out on any account. "The capacity gives you a hint of the confidence they have in their underwriting. If you ever want to go beyond that limit, you have to go somewhere else."

protecting your crown jewels

You can have the strongest firewall, the best IT team, and a crack network administrator, but none of these can guarantee that your network will always be secure and your critical files will remain intact. Despite your best efforts, a bored "script kiddie" could delete your product's source code, or a clumsy backhoe operator could inadvertently cut a fiber-optic line, bringing your business to a halt.

"Security is a process, not an event. It's not like fire, where you put in a sprinkler system and smoke detectors, and you're done. Your network is constantly in flux with new services, new employees, new operating systems and applications," says Scott Charney, principal at PricewaterhouseCoopers's cyber crime prevention and response group.

"Protect your crown jewels," he says. "Identify what you're trying to protect and the value of what you're trying to protect. This is risk mitigation, not risk elimination. You can't get down to zero risk. An e-policy will help you deal with the risk you cannot eliminate."

Schneier reminds clients that insurance is a risk management tool. "It turns a variable cost into a fixed cost," he says. "Businesses always like predictability, so insurance is a no brainer." ◘

Kevin has been a freelance computer technology writer for the past decade. Visit him at www.savetz.com.

Always use protection.

Before you send your files out into the world, see that they're protected. GlobalSCAPE's Secure FTP Server™ wraps your sensitive data with state-of-the-art security. Learn more. Visit **http://www.globalscape.com/sftp** and save 20%.

gObalSCAPE create. move. manage. / Makers of the Award-Winning CuteFTP Pro